UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,043	12/17/2001	David E. McDysan	RIC01059	5663

25537 7590 06/22/2007

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
06/22/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/023,043
Filing Date: December 17, 2001
Appellant(s): MCDYSAN, DAVID E.

Sangwon S. Kim
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 16 February 2007 appealing from the Office action mailed 24 July 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter as specifically presented in section V, pages 2-5, in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

U.S. Patent 5,768,271, issued to Seid et al.

Applicant Admitted Prior Art: paragraphs 04-11, and Figures 1 & 2

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 3-9, 11-16, and 18-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Seid et al. (U.S. Patent 5,768,271).

Referring to Claim 1:

Seid discloses a network system providing a virtual private network (VPN), said network system comprising:

one or more egress routers having connections to an access network including an access link (Figs. 1-3), wherein said one or more egress routers transmit intra-VPN traffic to a destination host belonging to the VPN from sources within the VPN within a first access network connection (e.g. elements 742-509 of Fig. 7) and all extra-VPN traffic to the destination host from sources outside the VPN within a second access network logical connections for extra-VPN traffic, separate from the first access network connection (Figure 7, particularly elements 25-39; and col. 4, lines 1-10); and

a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 2, line 56 – col. 3, line 15).

Referring to Claim 9:

Seid discloses a network system, comprising: an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); one or more egress routers having connections to the access network, wherein said one or more egress routers transmit intra-VPN traffic to the destination host via the first logical connection and transmit all extra-VPN traffic to the destination host via the second logical connection (Fig. 3; col. 8, lines 13-57); a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (Ibid, and also col. 7, line 62 – col. 8, line 13), such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Referring to Claim 16:

Seid discloses a method of providing a virtual private network (VPN), said method comprising: in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); communicating, from a plurality of ingress routers to one or more egress routers, intra-VPN and extra-VPN traffic destined for a destination host, wherein said

intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (col. 7, line 62 – col. 8, line 15); transmitting intra-VPN traffic from said one or more egress routers to the destination host belonging to the VPN via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress boundary routers to the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15), such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Referring to Claim 21:

Seid discloses a method for providing a virtual private network (VPN), the method comprising the steps of: intra-VPN traffic flowing from sources included in the VPN (Figure 7, and col. 4, lines 1-10); extra-VPN traffic flowing from sources outside the VPN (Ibid); assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to a destination host belonging to the VPN over traffic having the second priority level (col. 10, lines 40-65; col. 12, lines 20-30), transmitting intra-VPN traffic from said one or more egress routers to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one

or more egress routers toward the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15).

Referring to Claims 3 and 11:

Seid discloses the limitations of Claims 1 and 9 above. Seid further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers (col. 5, lines 40-60).

Referring to Claim 4:

Seid discloses the limitations of Claim 1 above. Seid further discloses further comprising the access network (Figs. 1-3).

Referring to Claims 5 and 12:

Seid discloses the limitations of Claims 4 and 9 above. Seid further discloses a customer premises equipment (CPE) edge router to the access link (col. 5, lines 40-60).

Referring to Claims 6, 13, and 18:

Seid discloses the limitations of Claims 5, 12 and 16 above. Seid further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (Figure 4).

Referring to Claims 7, 14, and 19:

Seid discloses the limitations of Claims 1, 9 and 16 above. Seid further discloses at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (col. 12, lines 20-30).

Referring to Claims 8, 15, and 20:

Seid discloses the limitations of Claims 1, 9 and 16 above. Seid further discloses said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic (col. 5, line 62 – col. 6, line 4).

Referring to Claim 22:

Seid discloses a method of communicating, comprising: receiving a packet that is destined for a host within a virtual private network (col. 9, lines 4-26); determining whether the packet is originated within the virtual private network or external to the virtual private network (col. 8, lines 21-23); and forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic originating externally to the virtual private network (col. 2, line 49 – col. 3, line 14; col. 8, lines 5-10).

Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seid.

Referring to Claim 23:

Seid discloses all the limitations of claim 22. Seid further discloses wherein the steps of receiving, determining, and forwarding the packet are performed at a customer premises router configured to process the packet (col. 5, lines 40-60; col. 8, lines 20-57) Although Seid does not explicitly mention the IP protocol or IP packets, Examiner takes Official Notice that it was well known in the art by the time the invention was made to transmit IP packets over the disclosed frame relay network hardware (see also Seid, col. 19. lines 48-57; for further reference consult the RFC 1490 reference below).

Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art (hereinafter, "AAPA") and further in view of Seid.

Referring to Claims 1, 9, and 16:

AAPA discloses a method of providing a virtual private network (VPN) comprising one or more egress routers having connections to an access network including the access link, wherein said one or more routers transmit intra-VPN traffic and extra-VPN traffic to the destination host belonging to the VPN (page 3, line 13 – page 5, line 20; Figures 1 and 2), and a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol (Ibid).

AAPA does not disclose wherein intra-VPN and extra-VPN traffic are separated into a first and second logical connection, nor that the logical connections are partitioned such that denial of service attacks on said access link originating from sources outside the VPN are prevented. However, Seid discloses a method for resisting denial of service attacks (i.e. network congestion, as taught by AAPA, page 5, lines 5-10) on any packet-switched network (col. 19, lines 48-57), comprising partitioning intra-VPN traffic and all extra-VPN traffic into a first and second logical connection (Figure 7, and col. 4, lines 1-10) in such a manner as to prevent denial of service attacks on said access link originating from sources outside the VPN (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition traffic between intra-VPN and extra-VPN sources as disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to allow a network to provide and maintain a level of service to a VPN that is unperturbed by other traffic on the network, in a manner superior to that offered by the prior art (Seid: col. 2, lines 43-46; AAPA: page 5, lines 14-20).

Referring to Claims 2, 10, and 17:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. AAPA further discloses wherein the at least one of the plurality of ingress routers or the at least one or more egress routers logically partitions intra-VPN traffic and extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic (AAPA: page 4, paragraph [09]).

Referring to Claims 3 and 11:

AAPA and Seid disclose the limitations of Claims 1 and 9 above. Seid further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers (col. 5, lines 40-60).

Referring to Claim 4:

AAPA and Seid disclose the limitations of Claim 1 above. Seid further discloses further comprising the access network (Figs. 1-3).

Referring to Claims 5 and 12:

AAPA and Seid disclose the limitations of Claims 4 and 9 above. Seid further discloses a customer premises equipment (CPE) edge router to the access link (col. 5, lines 40-60).

Referring to Claims 6, 13, and 18:

AAPA and Seid disclose the limitations of Claims 5, 12 and 16 above. Seid further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (Figure 4).

Referring to Claims 7, 14, and 19:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. Seid further discloses at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (col. 12, lines 20-30).

Referring to Claims 8, 15, and 20:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. Seid further discloses said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic (col. 5, line 62 – col. 6, line 4).

Referring to Claim 21:

AAPA discloses a known prior art method for providing a virtual private network (VPN), comprising assigning a first priority level to intra-VPN traffic flowing from sources included in the VPN (page 3, lines 1-11; page 4, line 14 – page 5, line 10); assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN (Ibid), and transmitting intra-VPN and extra-VPN traffic from one or more egress boundary routers to the destination host (page 3, lines 13-22; Figure 1).

It is unclear from AAPA whether the traffic having the first priority level at the access link is granted precedence of access to the destination host belonging to the VPN over traffic having the second priority level, nor that the intra-VPN and extra-VPN

traffic are transmitted over a first and second logical connections, respectively. However, Seid discloses the limitations regarding the priority levels (col. 10, lines 40-65; col. 12, lines 20-30) and the first and second logical connections (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition intra-VPN and all extra-VPN traffic in the manner disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to better prevent denial of service attacks from affecting intra-VPN traffic (col. 3, lines 10-15).

Referring to Claim 22:

AAPA discloses a method of communicating, comprising receiving a packet that is destined to a host within a virtual private network (page 2, paragraph 04), and determining whether the packet is originated within the virtual private network or external to the virtual private network (page 3, paragraph 06).

AAPA does not disclose "forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic originating externally to the virtual private network". However, Seid discloses these limitations (col. 2, line 49 – col. 3, line 14). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition intra-VPN and all extra-VPN traffic in the manner disclosed by Seid into the

network disclosed by AAPA. The motivation for doing so would be to better prevent denial of service attacks from affecting intra-VPN traffic (col. 3, lines 10-15).

Referring to Claim 23:

AAPA and Seid, disclose all the limitations of claim 22 above. AAPA discloses wherein the packet is an Internet Protocol (IP) packet (page 3, paragraph 06), and the steps of receiving, determining, and forwarding are performed at a customer premises router configured to process the IP packet (Ibid; see also Seid, col. 5, lines 40-60).

Referring to Claim 24:

AAPA and Seid, disclose all the limitations of claim 22 above. AAPA further discloses wherein the packet over the first logical path is marked at a higher priority that the second logical path using a differentiated services protocol (page 4, paragraph 09).

(10) Response to Argument

Examiner would like to begin by pointing out that Appellant's primary argument against the Seid reference is predicated upon a logical contradiction. On page 7 of the Appeal Brief, 2nd paragraph, Appellant describes the invention of claim 1 thusly:

> Specifically, the network system defined in independent claim 1 comprises, *inter alia*, first and second access network logical connections. The first access network logical connection is for intra-VPN traffic. **The second access network logical connection is for extra-VPN traffic**. The second access network logical connection is separate and apart from the first access network logical connection. **Both are within the VPN**.
> (emphasis Examiner's)

Careful analysis of Appellant's characterization of the instant invention reveals a paradox: the VPN contains traffic that by its very definition *cannot be part of the VPN*! (See the Advisory Action of 10/12/06, 1st paragraph of the continuation sheet regarding the definition of "extra-VPN traffic"). Having made this leap of logic, Appellant boldly presses on, by continuing to argue very emphatically that this "feature" is what distinguishes the instant invention over the prior art:

> "**In other words, traffic in a particular VPN is separated or partitioned based on the source of the traffic, i.e., whether the traffic originated within the VPN (intra-VPN) or outside of the VPN (extra-VPN)**" [page 7 of the Appeal Brief, 3rd paragraph, in re: the instant invention].

> "**Nothing, repeat nothing, is said** *[in the Seid reference]* **about segregating, within the same VPN, intra-VPN traffic from extra-VPN traffic**" [page 10 of the Appeal Brief, 1st paragraph, in re: the prior art].

(boldface emphasis Appellant's; underlined emphasis Examiner's)

Examiner respectfully submits that Appellant's argument is nothing more than a red herring, as there is neither any basis in the specification nor any recitation in the claims that **both** logical connections, and in particular the second logical connection comprising *extra*-VPN traffic, are part of the **VPN**. In order to make sense of Appellant's argument, it is necessary to consult the specification, which helpfully provides a clearer definition of the terms involved in the instant application. Examiner thus draws the Board's attention to the instant specification, page 10, paragraph 27, reprinted below with emphasis added:

> [27] To prevent traffic from outside a customer's community of interest (**e.g., traffic from other VPNs or the Internet at large**) from degrading the QoS provided to traffic from within the customer's community of interest (**e.g., traffic from other hosts in the same business enterprise**), the present invention either prioritizes intra-VPN traffic over extra-VPN traffic, or allocates access link capacity such that extra-VPN traffic cannot interfere

> with inter-VPN traffic. In other words, as described in detail below, each boundary router 22 gives precedence on each customer's access link to traffic originating within the customer's VPN, **where a VPN is defined herein as a collection of nodes coupled by a shared network infrastructure in which network resources and/or communications are partitioned based upon membership of a collection of nodes.** Granting precedence to intra-VPN traffic over extra-VPN traffic in this manner entails special configuration of network elements and protocols, including **partitioning of the physical access between intra-VPN and extra-VPN traffic using layer 2 multiplexing and the configuration of routing protocols to achieve logical traffic separation**. In summary, the configuration of the CPE edge router, the access network, the network-based VPN boundary router and the routing protocols involved in the edge and boundary routers cooperate to achieve the high-level service of DoS attack prevention, as detailed below. Conventional Diffserv and CPE edger router IPsec-based IP VPN implementations, by contrast, do not segregate traffic destined for sites within the same VPN (i.e., intra-VPN traffic) and traffic sent from other regions of the Internet (i.e., extra-VPN traffic).

Examiner believes that the flaw in Appellant's argument can now be more readily seen. The specification, and in particular the highlighted portions above, disclose that network resources [routers] partition traffic **over the physical access links** into intra-VPN traffic and extra-VPN traffic; indeed, this is exactly what is recited in exemplary claim 1. However, neither this passage nor any other portion of the specification teaches partitioning traffic **within a VPN** into intra-VPN and extra-VPN traffic, as argued by Appellant in the Appeal Brief. This is a subtle but significant distinction, for two reasons: (1) by definition, any traffic within a VPN is intra-VPN traffic, and therefore strictly speaking a segregation step would be trivial as there simply cannot be any extra-VPN traffic to filter out of the VPN; and (2) Examiner believes that Appellant has reinterpreted the term "VPN" to broaden its scope beyond what is actually disclosed or claimed. Appellant has erroneously concluded that the various routers employed by the instant invention are part of the VPN. *That is simply not true,* and betrays Applicant's garbled understanding of his own terminology. Indeed, exemplary claim 1 recites "a network system for providing a virtual private network (VPN)", and the specification teaches that

said network system can be the Internet itself (page 2 of the specification, paragraph 03). From Appellant's own argument in the Appeal Brief, it would then follow that any router on the Internet – and all traffic thereupon – would become a part of the VPN for purposes of the instant invention; but the previously quoted portion of the specification in paragraph 27 makes it clear that there is a difference between these types of traffic, *even though both types of traffic are handled by the same physical network resources*.

Clearly, Appellant's description of the primary issue under appeal does not reconcile with what Appellant previously disclosed in the specification, the claims, or even Appellant's summary of the subject matter presented earlier in the Appeal Brief! This bit of linguistic legerdemain serves only to confuse the true issue at hand. Based on the specification and the actual claim language, Examiner believes that Appellant intended to argue that Seid does not disclose segregating *within a [physical] access link*, intra-VPN traffic from extra-VPN traffic. But when viewed in this light, it becomes immediately apparent that Seid does, in fact, disclose the claimed functionality.

In order to see how the Seid reference reads on exemplary claim 1, it is first noted that Seid teaches "a network system providing a virtual private network", and even defines "VPN" in an equivalent manner to that found in Appellant's specification, seen for example in col. 2, lines 56-66, reprinted below with emphasis added:

> According to the present invention, in a packet switching (packet-based) network, such as a frame relay (FR) network, which includes network resources made up of networked elements and customer premises equipment interconnected by one or more physical paths, **a VPN is built above the underlying network and includes selected portions of the network resources. The VPN is a collection of logical nodes and virtual paths (VPs) and includes one or more virtual circuits (VCs), each VC being a logical connection between VC terminators including network elements and customer premises equipment**.

Seid discloses wherein a VPN includes both physical network elements as well as logical connection elements: Virtual Paths (VPs) and Virtual Circuits (VCs), defined in col. 5, lines 40-60 for example. As seen in Figure 4 and in col. 6, lines 30-48, VCs represent a second, additional layer of abstraction for network traffic over and above the VPs of the network. Thus, for purposes of mapping the prior art to the claims, one need only consider the VPs as corresponding to the "access network logical connections" recited in the claims. VCs are only pertinent to the claimed subject matter insofar as knowledge of a particular VC and VP is required to identify the specific VPN to which a given packet of network data belongs (Seid, col. 7, lines 5-15).

On page 8 of the Appeal Brief, third paragraph, Appellant tries to draw an artificial and non-existent distinction between the instant invention and the prior art: namely, that "packets to different VPNs are identified, but not on the basis of whether they originated within a particular VPN or without a particular VPN". This is incorrect; Seid discloses that, during the process by which a VPN is created, the endpoints for all VPs to be used in said VPN must be defined in advance, and that each VP must be identified to belong to one specific VPN (Seid, col. 15, lines 10-25). From this passage, it is evident that if one can identify at least the VP to which a VPN packet belongs, then it necessarily follows that it originated from an endpoint also known to belong to said VPN. Additionally, Seid also discloses that standard FR traffic (i.e. non-VPN traffic) can similarly be identified and routed appropriately, on its own logical connection (Seid, col. 8, lines 50-60; further noting that **all** non-VPN traffic shares a single logical connection as disclosed in col. 13, lines 1-3).

Examiner notes that Appellant's argument above suggests that Appellant continues to believe that Seid discloses wherein traffic that was originally designated as belonging to one VPN is somehow altered so as to be delivered to a different VPN, an argument was made in the Amendment after Final of 9/25/06. Examiner submits that, if the traffic designated for one VPN (as identified by its unique combination of VPs and VCs: again see Seid, col. 15, lines 10-25) were somehow transmitted to a different VPN (with its own unique combination of VPs and VCs), this would represent a malfunction of the disclosed system. Examiner repeats his request from the Advisory Action of 10/12/06, 2nd paragraph, for Appellant to provide some evidence from the Seid text that supports Appellant's unsubstantiated allegation wherein Seid discloses transmitting traffic from one VPN to another VPN.[1] In the words of the Appellant from page 8 of the Appeal Brief, "**Where? If only saying so could make it so**."

The network system provided by Seid provides one or more egress routers and a plurality of ingress routers, in the form of a series of network nodes as illustrated in Figures 2 and 3, and defined in col. 5, lines 40-60. Herein, it is illustrated that each every node in the network is capable of bidirectional traffic: network node A is capable of sending data to and receiving data from Customer Premises Equipment 1, and network node B is capable of sending data to and receiving data from Customer Premises Equipment 2. Furthermore, each node disclosed by Seid is capable of routing traffic as appropriate (see Seid, col. 7 lines 5-10; in more detail at col. 8, lines 14-57).

[1] Examiner notes in advance that Seid's references to "cross-connect nodes" fails to support Appellant's original argument, as said cross-connect nodes do not refer to crossing VPNs but rather crossing among VPs within the same VPN (Seid, col. 6, lines 49-55). In fact, cross-connect nodes are invisible to VPNs (Seid, col. 14, line 43-45).

This clearly conforms to the instant specification's definitions of "ingress router" and "egress router" as found in paragraph 06 of the specification on page 3 and paragraph 11 on page 5, reproduced here with emphasis added:

> [06] FIG. 1 illustrates the implications of utilizing a conventional Intserv implementation to perform admission control. As shown in FIG. 1, an exemplary IP network 10 **includes N identical nodes (e.g., service provider boundary routers) 12, each having L links of capacity X coupled to Customer Premises Equipment (CPE)** 14 for L distinct customers. In a per-flow, connection-oriented approach, each node 12 ensures that no link along a network path from source to destination is overloaded. Looking at access capacity, a per-flow approach is able to straightforwardly limit the input flows on each of the ingress access links such that the sum of the capacity for all flows does not exceed the capacity X of any egress access link (e.g., Link 1 of node 12a). A similar approach is applicable to links connecting unillustrated core routers within IP network 10.
>
> [0011] FIG. 2 depicts a DOS attack scenario in an exemplary IP network 10' that implements the conventional Diffserv protocol. In FIG. 2, **a number of ingress nodes (e.g., ingress boundary routers) 12b'-12d' each admit traffic targeting a single link of an egress node (e.g., egress boundary router) 12a'. Although each ingress nodes 12' polices incoming packets to ensure that customers do not exceed their subscribed resources at each DSCP, the aggregate of the admitted flows exceeds the capacity X of egress Link 1 of node 12a', resulting in a denial of service to the customer site served by this link.**

Thus once again referring back to Seid, from the above it can be seen that at least Nodes A and B comprise both the "one or more egress routers" and "plurality of ingress routers" recited in the claims.[2] Furthermore, Seid also discloses in a related aspect of that invention an exemplary configuration of a single VPN wherein a plurality of ingress routers D_1 through D_n all transmit traffic to a single egress router S, while employing the logical partitioning of traffic to ensure that the egress access link will never exceed the bandwidth limit of Y kbps regardless of excess traffic/congestion from multiple sources (see Seid, Figure 10, and col. 19, lines 33-37). It must be noted at this point that the

[2] It is noted that the instant specification only refers to "ingress routers" and "egress routers" in describing the Applicant Admitted Prior Art; embodiments of the instant invention refer instead to "edge routers" and "boundary routers" in describing the equivalent functionality of the instant invention.

scenario where the egress link's bandwidth is overwhelmed by excessive traffic from multiple sources is *precisely* how the instant specification defines "denial of service attack" (see paragraph 11, quoted above); which Seid clearly prevents.

Before clarifying how Seid discloses the limitations regarding logical partitioning of traffic, it is worth noting that the instant specification explicitly defines "extra-VPN traffic" as "traffic *from other VPNs* or the Internet at large" (page 6, paragraph 13 and page 10, paragraph 27; the latter having already been quoted on pages 14-15 of this Answer). Appellant's argument is structured in a way as to imply that the claim is limited only to a network system with exactly one VPN would be covered by the claims; but such a limited interpretation is not supported by the instant specification.[3]

Seid discusses in great detail about how precisely traffic management and congestion control operate within that invention, beginning at col. 10, line 11, and proceeding through at least col. 12, line 52. Some particularly relevant passages are reprinted below, with emphasis added:

Col. 10, lines 20-30:

> The forward congestion notification processing, e.g., the notification of congestion to a destination of a data stream, is handled analogously. **The VPN of the present invention provides improved traffic management and congestion control because traffic associated with a specific VPN is uniquely identified within the FR network. Therefore, the traffic management and congestion control in accordance with the invention is implemented such that the traffic within a given VPN is unperturbed by traffic generated outside of the VPN's logical domain**.

[3] Appellant has also made this argument before, without success: see the Amendment after Final filed 9/25/06, page 8, bottom paragraph; cf. Advisory Action of 10/12/06, page 3, 1st paragraph.

Seid teaches that one of the novel aspects of the invention is the very ability to uniquely identify VPNs (and as seen previously, non-VPN traffic can also be identified in the same manner), for the purpose of allowing one or more VPNs to function without regard to traffic outside of said one or more VPNs' logical domain(s). It is also worth noting that this paragraph describes an aspect of the Seid invention wherein there exists but a single VPN on the network ["the VPN of the present invention"], and is clearly capable of distinguishing traffic belonging to said VPN [i.e. intra-VPN traffic] from traffic belonging to the FR network in general [i.e. extra-VPN traffic, using Appellant's preferred narrow interpretation of the term]. Also observer that "traffic generated outside of the VPN's logical domain" [i.e. "from sources outside the VPN", as per the claim language] will not adversely impact the traffic of the VPN of the Seid invention.

Col. 10, lines 38-50:

> The role of congestion management at the Phy-sap in accordance with the invention is to ensure that each VP is allocated at least VP-CIR for data transmission over the trunk (PP). **Therefore, if congestion occurs on the PP, there will be sufficient bandwidth such that each VPN can at least transmit traffic at VP-CIR on the PP**. If a PP is carrying FR traffic other than VP traffic, the total allocated bandwidth on the PP must ensure that each VP is guaranteed at least VP-CIR. Therefore the sum of each VP-CIR and CIR for other FR traffic on the trunk must not exceed the total bandwidth of the PP. **If congestion occurs, then only those VPs (or other FR traffic) in excess of their corresponding CIRs must reduce submission rate onto the PP**.

Here, Seid explicitly discloses an embodiment wherein on a given physical link traffic not belonging to any VPN ["other FR traffic"] will be throttled while simultaneously permitting one or more VPNs to continue using their allotted bandwidth ["VP-CIR"] unimpeded when congestion is detected. Examiner wishes to repeat that Seid does in

fact disclose embodiments where there exists exactly one VPN overlaid on a physical network capable of carrying standard FR traffic (see Figure 10 for example).

And col. 12, lines 20-30 (this was also cited for claims 7, 14, and 19):

> As discussed above with respect to a single integrated address field, an ingress VP identity for the incoming frame is given by the field ivpi in the connection table. The VP concept allows the isolation of traffic of one user (or VPN) from the traffic of another user (or VPN). **As will be understood by those skilled in the art, one VP, VP_i, can be congested while another VP, VP_k, sharing the same trunk is not congested.** Simultaneously, the configuration of the invention allows a (non-congested) user to have a VP SR higher than the VP-bandwidth it has reserved. This situation occurs when the network is not heavily loaded.

This is perhaps the clearest instance yet of the disputed limitation: an explicit disclosure of two logical connections (VP_i and VP_k) over the same access link (the trunk, see col. 7, line 55 for clarification). Thus, in this specific example, the disclosed (non-congested) user will receive his intra-VPN traffic via the logical connection VP_k, without congestion, while a second VPN with a second logical connection (VP_i) over the same physical access link carrying extra-VPN data to the same destination host[4] simultaneously experiences congestion ["denial of service attack"].

Examiner also wishes to note an inconsistency in Appellant's characterization of the Seid reference. On page 10 of the Appeal Brief, 2nd paragraph, Appellant describes the Seid invention thusly:

> Instead of facing up to that fact, the Examiner attempts to misdirect attention to the overall objective of Seid et al. **which is to control congestion within each VPN**. [emphasis Examiner's]

[4] Seid teaches that one of ordinary skill in the art would have known that a host can be a member of multiple VPNs simultaneously: see Figure 1, node A and the node comprising VPN4.

But in the very next paragraph, Appellant characterizes Seid differently:

> In short, Seid et al. merely distinguish VPNs to isolate traffic **from one VPN to another VPN** to control congestion. [emphasis Examiner's]

Examiner respectfully requests that Appellant clarify what exactly Appellant believes to be the purpose of the Seid reference: does Seid teach controlling congestion within the same VPN or to prevent one VPN's traffic from negatively impacting traffic of another VPN?[5] While Examiner admits that one of the advantages of the Seid invention is the ability to control congestion within each VPN (see col. 19, line 33-47), it is **NOT** the only purpose of that invention; as has now been repeatedly established, Seid *also* prevents congestion ["denial of service attacks"] of one logical connection from causing harm to another logical connection (e.g. col. 12, lines 20-30).

Examiner submits that the Seid reference, including but not limited to the passages quoted herein, clearly disclose and anticipate Appellant's invention as recited in claim 1. Additionally, while the arguments presented herein were directed to the rejection of the claims under 35 USC 102(b)[6], they are equally applicable to the obviousness rejections under 35 USC 103(a) in view of the combination of Applicant Admitted Prior Art with Seid. Once again, Seid discloses the ability to partition traffic on a packet-switched network in order to provide logical connections for each of one or more VPNs, as well as a separate logical connection for all non-VPN traffic, in such a

---

[5] Examiner has found it difficult to formulate an unequivocal Answer to the appeal brief in view of the Appellant's inconsistencies in describing Appellant's understanding of not only the prior art but also the instant invention itself (cf. pages 13-16 of this Answer).

[6] For purposes of this discussion, the rejection of claim 23 over 35 USC 103(a) in view of Seid alone stands or falls with the 102 rejections, and is traversed with substantially similar reasoning.

way as to ensure that traffic within a given VPN (via its logical connection) is unperturbed by traffic generated from outside the VPN's logical domain (Seid, col. 10, lines 20-30); consequently, it would have been obvious to one of ordinary skill in the art to apply the logical connection partitioning techniques of Seid to the previously disclosed packet switched network admitted by the Applicant for the reasons discussed above and in the previous Office Action(s). Thus, Examiner respectfully requests that the Board uphold all the rejection(s) of claim 1 over the prior art for at least the reasons discussed above.

As Appellant has argued that claims 1-24 stand or fall as a group with claim 1, thus Examiner respectfully submits that all rejections of claims 1-24 should also be upheld for at least the reasons discussed above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Thomas Gyorfi TG

Examiner, Art Unit 2135

Conferees:

Kim Vu KV

Supervisory Examiner, Art Unit 2135

Taghi Arani TA

Primary Examiner, Art Unit 2139